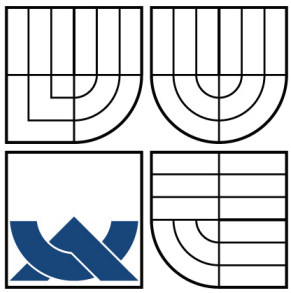
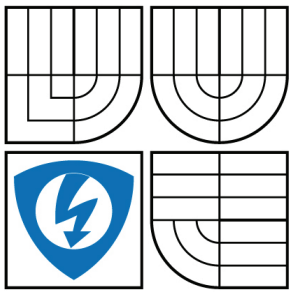


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

METODY KVANTOVÉ KRYPTOGRAFIE

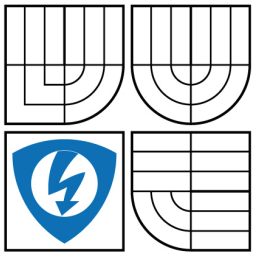
QUANTUM-BASED CRYPTOGRAPHY METHODS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — MÁRIA PAJTINOVÁ
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. VÁCLAV ZEMAN, Ph.D.
SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Studentka: Mária Pajtinová ***ID:*** 78434
Ročník: 3 ***Akademický rok:*** 2008/2009

NÁZEV TÉMATU:

Metody kvantové kryptografie

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se a stručně popište metody využívané v kvantové kryptografii. Zaměřte se především na protokoly umožňující bezpečnou výměnu šifrovacích klíčů prostřednictvím otevřeného komunikačního kanálu. Dále proveďte průzkum současného stavu komerčních technických zařízení založených na kvantových kryptografických mechanismech.

DOPORUČENÁ LITERATURA:

[1] FORMÁNEK J. : Úvod do kvantové teorie. ACADEMIA, Praha 2004.
[2] SINGH, S.: Kniha kódů a šifer. Dokořán, 2002, ISBN 8086569187

Termín zadání: 9.2.2009 ***Termín odevzdání:*** 2.6.2009

Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

Abstrakt

Bakalářská práce analyzuje metody kvantové kryptografie, konkrétně popisuje používané přenosové protokoly využívající otevřený komunikační kanál. Tyto metody prakticky předvádí simulační program, který je součástí. V další části práce je provedený průzkum v současnosti vyráběných zařízení využívající kvantovou kryptografii.

Klíčová slova

Kvantová kryptografie, Kvantová distribuce klíče, Protokol BB84, Protokol B92, Šestistavový protokol, EPR protokol, Protokol SARG04

Abstract

Bachelor‘s thesis analyzes quantum-based cryptography methods, specially there are described mostly used transport protocols of QC based on open communication channel. These methods are practically explained by simulation program, that is included,. In another section, corporations research concerned on quantum cryptography and communication are performed.

Keywords

Quantum Cryptography, Quantum Key Distribution, Protocol BB84, Protocol B92, Six-state protocol, EPR protocol, Protocol SARG04

PAJTINOVÁ, M. Metody kvantové kryptografie. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 49 s. Vedoucí bakalářské práce doc. Ing. Václav Zeman, Ph.D.

Prohlášení

Prohlašuji, že svou bakalářskou práci na téma *Metody kvantové kryptografie* jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestně právních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

Poděkování

Děkuji vedoucímu bakalářské práce doc. Ing. Václavu Zemanovi, Ph.D.za jeho cenné rady a nápady, které vedli ke zdokonalení mé práce.

V Brně dne ....

Obsah

Úvod

Už dlouhou dobu se lidé snažili přijít na způsob, kterým by mohli komunikovat prostřednictvím zpráv tak, aby si byli 100% jisti, že jejich zprávu dostane pouze oprávněný příjemce. Z toho důvodu vznikla věda s názvem kryptografie. Nedávno po jejím vzniku však vznikla druhá věda – kryptoanalýza, která se, naopak, zaobírala luštěním těchto zpráv. A tak se strhl pomyslný boj kryptografů a kryptoanalytiků, díky kterému vznikali neustále nové způsoby šifrování zpráv a jejich následné rozluštění.

Při šifrování zpráv je nejdůležitějším článkem tajný klíč, který musí znát odesílatel i příjemce. Při jeho znalosti je triviální přečíst zcela nelogickou zprávu. Ještě před samotným šifrováním je potřeba doručit tento klíč odesílateli, a zde vyvstává obrovský problém. Je možnost klíč doručit osobně, ale na větší vzdálenosti je toto docela nevhodné a finančně i časově náročné. Další možností je odeslání tohoto klíče poštou nebo kurýrem, ale v tomto případě si zas nemůžeme být zcela jisti, jestli se klíč dostane právě a jen k uvedenému adresátovi. Tento problém by mohl vyřešit nejmladší vědní obor kryptografie, kterým je kvantová kryptografie. Tato vědní disciplína se nezaobírá samotným šifrováním, ale pouze přenosem klíče na základě vlastností kvantové fyziky.

Tato práce pojednává o výše zmíněné oblasti kryptografie, obsahuje podrobný popis jejich metod i názorné příklady, jak u jednotlivých protokolů distribuce klíče probíhá. Součástí bakalářské práce je také vytvořený program, který simuluje přenos klíče u jednotlivých kryptografických protokolů. V další části byl proveden průzkum společností zabývajících se kvantovými technologiemi, který ukazuje praktické využití této vědné disciplíny.

1. Teoretické východiska kvantové kryptografie

Na začátku této práce bych ráda objasnila základní pojmy, které se týkají kvantové kryptografie, konkrétně kryptografie a kvantové fyziky.

1.1 Kryptografie a její historie

Kryptologie je vědní disciplína, která se zabývá utajením a odhalením zpráv a dělí se na dvě části, na kryptografii a kryptoanalýzu. U kryptografie jde o nacházení a popis metod utajení zpráv pomocí šifer. V minulosti se používala zejména k vojenským nebo státním účelům, nyní je součástí každodenního života kohokoli z nás. Pod pojmem šifra si představíme algoritmus, pomocí kterého srozumitelné zprávy zpráva šifrovaná, neboli nečitelná pro osobu neznalou klíče. Kryptoanalýza je naopak nauka o luštění těchto zpráv bez znalosti klíče, pomocí nalezení slabého místa v šifře tak, aby byl zašifrovaný text rozluštěn. Slovo klíč v tomto pojetí znamená sled znaků nebo slov, pomocí kterých je možno zašifrovaný text přečíst.

Počátky kryptografie se datují do dob kolem 5. století před naším letopočtem. Už v tomto období bylo důležité domlouvat se na dálku se svými spojenci bez toho, aby byl nepřítel schopen rozluštit vzkaz. V této době se používala zejména steganografie, což je věda, která se věnuje utajení zpráv jejich ukrytím. Tato technika má však jednu obrovskou nevýhodu. Po jejím odhalení je hned odkryt celý text, a to je důvod, proč se začala rozvíjet kryptografie.

Klasická kryptografie využívá dvou způsobů šifrování: transpozice (přeuspořádání písmen) a substituce (nahrazování písmen jinými). Druhý způsob byl základem Caesarovy posunové šifry navržené Juliem Caesarem, kde bylo každé písmeno nahrazeno písmenem posunutým o několik pozic v abecedě. V tomto případě byl klíč číslo v rozmezí 1 až 25 (počet písmen v abecedě je 26), o kolik byla posunutá abeceda. Tato šifra však byla poměrně slabá a brzy byla prolomená. Její bezpečnější obměnou byla monoalfabetická substituční šifra, ve které šifrování spočívalo v tom, že každému písmenu bylo přiděleno jiné v nezvyklém pořadí, příp. i s využitím klíče. Kryptoanalytici našli slabinu i v této šifře, když použili tzv. frekvenční analýzu, která předpokládá četnost pravděpodobného výskytu písmen v abecedě. Díky této četnosti je možno rozluštit nejfrekventovanější písmena abecedy a zbytek doplnit podle kontextu. Kryptografové však nezaháleli a snažili se přijít na způsob, který by zaručil absolutní bezpečnost.

V 15. století se poprvé objevuje tzv. neprolomitelná šifra, jejíž objevitelem byl Blaire de Vigenère. Ta měla kořeny v šifře monoalfabetické, avšak jednomu znaku otevřeného textu mohlo náležet více znaků šifrovaného textu. To znamená, že byla vůči četnosti zcela odolná, protože každé písmeno bylo zašifrováno pomocí jiného posunu v abecedě. Vzhledem k tehdejší téměř úplné dokonalosti je neuvěřitelné, že dvě století byla tato šifra zcela ignorována. Po čase však analytici našli slabinu i v této šifře.

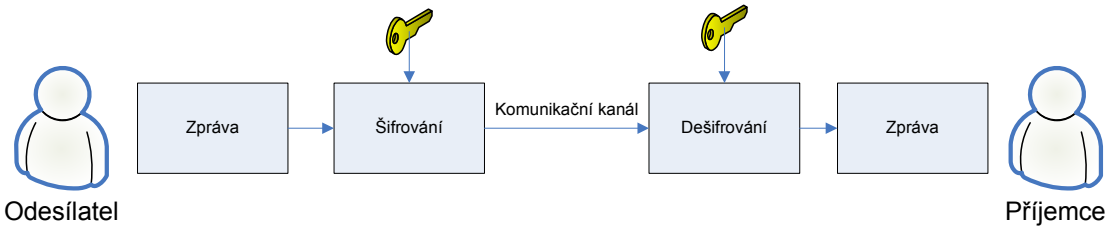
V roce 1917 si nechal Gilbert Vernam patentovat metodu šifrování s názvem Vernamova šifra, také známou pod pojmem One-time pad. Zakládala se na posunu abecedy o předem náhodně vygenerované čísla, které tvořili klíč. Tato je ve svém důsledku za daných okolností neprolomitelná, co je způsobeno následujícími skutečnostmi: klíč je stejně dlouhý jak přenášená zpráva, zcela náhodný a je možno ho použít pouze jednou. Tato neprolomitelnost byla vědecky prokázána v roce 1949 Američanem Claudem E. Shannonem. Největším nedostatkem této šifry je problém distribuce klíče, a z tohoto důvodu se využívala velice zřídka [10]. O několik desetiletí tento problém vyřešil objev kvantové kryptografie, která Vernamovu šifru plně využívá.

Vzhledem k tomu, že 1. světová válka byla ukončena kapitulací Německa z důvodu odhalení tajné korespondence, německý vynálezce Arthur Scherbius se snažil dosáhnout náhradu zastaralých šifrovacích systémů moderními technologiemi. Tak byla vynalezena Enigma, přístroj, který se skládá z pěti částí: klávesnice pro psaní textu, propojovací desky, tří rotujících vyměnitelných šifrovacích jednotek – scramblerů, reflektoru a desky, na které se zobrazoval šifrovaný text. Bez klíče, pomocí kterého se dalo text rozluštit, by nepřítel musel vyzkoušet celkově 10^{16} možností na dešifrování zprávy. Zpočátku se Enigma příliš neuplatnila kvůli vysoké ceně a nedůvěryhodnosti, avšak po zjištění, že britská vláda rozluštila tajnou komunikaci, německá armáda začala tento stroj masově používat. Od dob 2.světové války byla Enigma považována za dokonalý šifrovací mechanizmus, který není možno dešifrovat. O 30 let později ovšem vyplulo na povrch, že britské dešifrovací jednotky přišli na způsob, jímž bylo možno dešifrovat vojenskou konverzaci.

V padesátých letech 20. století se začala rozvíjet éra počítačů, díky nímž bylo šifrování mnohem rychlejší, šifry složitější, ale bylo vymezeno jen pro vládu a armádu, které jako jediné počítače vlastnili. V roce 1976, kdy byli počítače běžně dostupné podnikatelským subjektům a důraz byl kladený hlavně na bezpečnost, byl přijat americký standard pro šifrování DES (v současnosti nahrazen standardem AES).

S rozvojem počítačů se zrodil obrovský problém, šifry sice byly dostatečně bezpečné, ale pro jejich dešifrování bylo potřeba nejdřív distribuovat klíč. Tento zádrhel se podařilo vyřešit trojici amerických výzkumníků Ronaldu Rivestovi, Adimu Shamirovi a Leonardu Alemanovi. Tito jsou vynálezci první asymetrické šifry RSA, která byla založena na principu jednosměrné funkce (konkrétněji násobení prvočísel v modulární matematice), čímž byla umožněna existence veřejného a soukromého klíče. Obtížnost útoku na tuto šifru roste s velikostí jejího klíče exponenciálně, nicméně v roce 1999 se podařilo prolomit šifru RSA s délkou klíče 512bitů [19]. Z této metody později vycházel Phil Zimmermann, autor šifrovacího softwaru PGP, který používal současně symetrickou i asymetrickou šifru a umožnil široké veřejnosti výrazně větší soukromí [28].

V současné době používají kryptografové algoritmy, které dělíme na symetrické a asymetrické. Největší rozdíl tkví v tom, že symetrické algoritmy využívají pro šifrování i dešifrování zprávy stejný tajný klíč, který musí znát odesílatel i příjemce. Standardní postup tohoto šifrování je znázorněn na obr. 1.1. Na druhou stranu, u asymetrických algoritmů jsou potřebné 2 klíče – soukromý a veřejný. Princip spočívá v tom, že veřejný klíč, který slouží k šifrování (může být zveřejněn, kupříkladu na internetu) je schopen získat kdokoli, ale zašifrovanou zprávu dokáže přečíst pouze určený příjemce, který zná soukromý klíč.



Obr. 1.1: Princip symetrických algoritmů

V současné době jsou asymetrické algoritmy v kombinaci se symetrickými dostatečně silné a výkonné, aby zaručily uspokojivou úroveň utajení, ale je jen otázkou času, kdy budou vyvinuty výkonnější kvantové počítače, které budou schopny rozluštit tyto šifry během pár chvil. Řešením tohoto problému může být zavedení mechanizmů kvantové fyziky do systému distribuce klíče s použitím symetrických šifer.

1.2 Kvantová fyzika

Hlavní rozdíl mezi kvantovou a klasickou fyzikou tkví v tom, že v klasické fyzice jsme schopni přesně změřit kteroukoli veličinu, přičemž vliv měření lze

jednoduše minimalizovat. Naopak u kvantové fyziky nejsme schopni změřit v určitých kvantových stavech některé veličiny, z čeho vyplývá, že při opakovaných měřeních dostaneme rozdílné výsledky a kvantové měření stav systému ovlivní.

Podle korpuskulární teorie se částice mohou chovat jako vlny a naopak. Max Planck vyslovil domněnku, že při přenosu světla atomem je energie dodávána po kvantech. Elementární částice záření, kterou popisujeme kvanta světla, je označována jako foton, který je nejdůležitějším prvkem v kvantové kryptografii.

Dalším důležitým termínem je polarizace fotonu, na tomto principu pracují všechny protokoly kvantové kryptografie — QC. Polarizace znamená výběr jen jedné kmitové roviny elektromagnetického vlnění ze všech možných, což značí, že „… fotony jako kvanta příčného elektromagnetického vlnění mohou mít dvě nezávislé polarizace. Skutečný stav fotonu je potom lineární kombinací obou polarizačních stavů v dané bázi.“ [16] Pro její měření se používá polarizační hranol. Skládá se ze 2 vybroušených monokrystalů (nejčastěji z islandského vápence). Natáčením hranolu můžeme měřit fotony ve 2 rovinách — bázích, a to lineární (horizontální a vertikální), nebo diagonální (posunutí lineární roviny o 45° nebo 135°). Při správném natočení můžeme přesně určit polarizaci. Důležité ale je, že při nesprávné volbě báze není možno zjistit polarizaci fotonu, která se náhodně změní vzhledem k tomu, že báze nejsou kompatibilní. Tato myšlenka je popsána Heisenbergovým principem neurčitosti, který říká, že čím přesněji změříme u částice polohu *r*, tím nepřesněji určíme její hybnost *p* a naopak, i při použití sebelepších přístrojů. Tyto veličiny jsme zvolili právě proto, že patří do skupiny nekomutujících, čili jsou kvalitativně různé, ale neumožňují kompletní popis kvantově mechanického systému. Tento princip můžeme popsat vztahem

$$\Delta x \cdot \Delta p \geq \hbar, \tag{1.1}$$

kde Δx a Δp jsou neurčitosti pro měření x-ových složek *r* a *p*, ħ je redukovaná Planckova konstanta s hodnotou

$$\hbar = \frac{h}{2\pi} = \frac{6{,}63 \cdot 10^{-34}}{2\pi} = 1{,}054 \cdot 10^{-34}\,[\mathrm{J \cdot s}], \tag{1.2}$$

zde h značí Planckovu konstantu. Předpokládejme, že na částici nepůsobí žádná síla, její hybnost *p* je tedy konstantní. Přitom předpoklad je, že hybnost této částice je možno

přesně určit a že $\Delta p = 0$, to by znamenalo, že $\Delta x \rightarrow \infty$. Vzhledem k nekonečně velké neurčitosti není možno určit polohu částice *r* [11].

U dvoučásticového protokolu se setkáme s tzv. EPR paradoxem. Tento myšlenkový experiment je nazván po svých zakladatelích Albertu Einsteinovi, Borisovi Podolskem a Nathanovi Rosenovi. Pojednává o tom, že kvantová mechanika není úplná teorie a není schopna popisovat fyzikální realitu. Nechť jsou dvě částice, které jsou ve stavu kvantové provázanosti a na začátku tvoří pár. Po jejich rozdělení se vzdálí na libovolnou vzdálenost. Když změříme první částici v jedné ose, v ten samý moment můžeme změřit druhou částici s tím, že víme, že oproti první bude mít opačnou hodnotu. Tady nastává nesrovnalost, protože měření jedné částice je zcela náhodné, a přesto může ovlivnit hodnotu druhé, která s ní není ve fyzikálním kontaktu. Z těchto pokusů Einstein usoudil, že existují skryté proměnné s doposud nepopsanými vlastnostmi, které by byli schopny popsat toto chování [20].

Skryté proměnné se úspěšně pokusil popsat v roce 1965 John Bell. Představme si, že máme pár fotonů a pootočením dvou polarizačních hranolů o několik stupňů chceme změřit jejich polarizaci. Tyto uhly můžeme zvolit např. u prvního hranolu jako $\alpha = 0^{\circ}$, při kterém naměříme hodnotu +1, $\alpha' = 45^{\circ}$ hodnotu -1, u druhého hranolu $\beta = 112{,}5^{\circ}$ s hodnotou +1 a $\beta' = 67{,}5^{\circ}$ s hodnotou -1. Tyto hodnoty předem neznáme, ale někteří zastánci skrytých parametrů tvrdí, že jsou předem určeny a dány určitým skrytým parametrem. Sestavíme si následující rovnici s tím, že γ bude určovat střední hodnotu dat

$$\gamma = \alpha\beta + \alpha\beta' + \alpha'\beta - \alpha'\beta'. \tag{1.3}$$

Dosazením všech možných úhlů zjistíme, že γ může nabývat hodnot od –2 do +2. Dosazením hodnot do výše zmíněné rovnice dostaneme

$$< \alpha\beta > + < \alpha\beta' > + < \alpha'\beta > - < \alpha'\beta' > = -\cos(225°) - \cos(135°) - \cos(135°) +$$

$$\cos(45°) = 2\sqrt{2}. \tag{1.4}$$

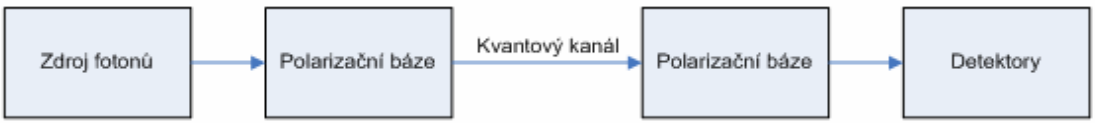
Vzhledem k tomu, že $2\sqrt{2} > 2$ nastává jev, kdy kvantová mechanika Bellovy nerovnosti porušuje [4].

2. Protokoly kvantové kryptografie

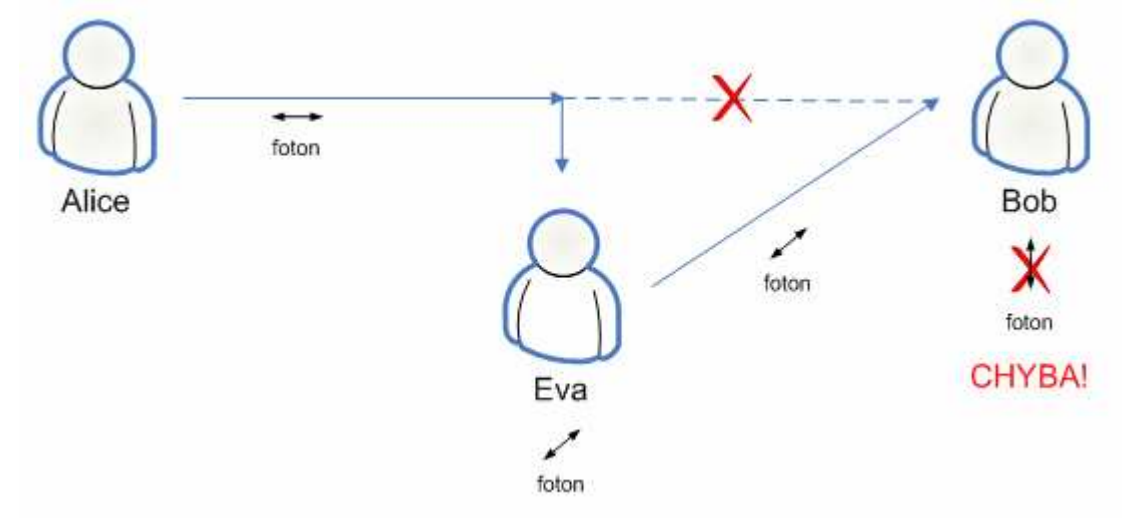
Klasická kryptografie se zaobírá šifrováním zpráv, přičemž tyto úkony se zakládají pouze na matematických operacích. Naproti tomu v kvantové kryptografii jde pouze o systém distribuce klíče (Quantum Key Distribution - QKD) (obr. 2.1) s využitím zákonitostí přírody, konkrétně kvantové mechaniky. Její bezpečnost stojí hlavně na několika kvantových poznatcích, a to nemožnost rozdělit jeden foton na více částí, nemožnost tento foton replikovat bez toho, aby byla některá jeho vlastnost změněna a nemožnost měření určitých veličin zároveň [21]. Bity klíče jsou kódovány pomocí kvantových stavů fotonů. Každý foton nese v tomto případě právě jeden bit nazývaný též qubit (kvantový bit), který může nabývat hodnoty 1 nebo 0. Po bezpečném doručení klíče následuje klasické šifrování, například pomocí symetrické Vernamovy šifry.

V následujících částech budou chronologicky vysvětleny protokoly, které už bylo možno provést i prakticky, i když jen na malé vzdálenosti přes optický kabel a s nízkou přenosovou rychlostí.

V kryptografii vystupují většinou tři fiktivní osoby – Alice, Bob a Eva. Alice a Bob vystupují jako strany se zájmem o bezpečnou komunikaci a Eva jako útočník, který se jí snaží prolomit (obr. 2.2). Alice by chtěla odeslat zprávu Bobovi, ale je potřeba se nejdřív domluvit na klíči, pomocí kterého bude zpráva zašifrována kvůli možnému odposlechu Evou. Tímto vyvstává problém bezpečné distribuce tohoto klíče. Je možno se osobně setkat a předat si klíč, ale na větší vzdálenost nebo ve větším množství je tato možnost docela nepraktická. Dále bychom mohli odeslat klíč kurýrem, co taky není zrovna vhodná volba z důvodu financí nebo odchycení klíče Evou. Tento problém je možno vyřešit díky kvantové kryptografii [28].



Obr. 2.1: Obecný postup kvantového převodu informací



Obr. 2.2: Přenos klíče v podobě fotonu za přítomnosti Evy

2.1 Protokol BB84

Čtyřstavový protokol BB84 byl navržen v roce 1984 americkými vědci Charlesem H. Bennettem a Gillesem Brassardem, po nichž byl tento protokol pojmenován. Tito vycházeli z námětu Stephena Wiesnera, který navrhl nepadělatelné kvantové peníze, které ale nebylo možné zkonstruovat, a proto jim nikdo nevěnoval pozornost.

Protokol BB84 nejčastěji využívá lineární a diagonální polarizaci fotonů, ale lze využít i kruhovou. Polarizaci fotonů můžeme provádět ve dvou polarizačních bázích – lineární, značíme „+“ (odkloněná od vertikály o 0˚ nebo 90˚) a diagonální, značíme „×“ (odkloněná od vertikály o 45˚ nebo 135˚). Podrobnosti generování a vyhodnocování fotonů jsou obecně známé a lze je najít např. v [12].

V nejjednodušším případě použijí Alice a Bob pouze jednu bázi a podle předešlé dohody zakódují třeba horizontálně polarizovaný foton do hodnoty 0 a vertikálně polarizovaný do hodnoty 1. Bob by pak tyto fotony nechával procházet polarizačním hranolem, který by mu přesně určil podle průchodu nebo odrazu tímto hranolem jeho hodnotu. Tento způsob komunikace by nebyl příliš bezpečný, protože kdyby odposlouchávající Eva uhodla bázi, na které se Alice s Bobem dohodli, dokázala by určit klíč bez toho, aby si odposlechu někdo všiml.

Pro větší bezpečnost se proto používají báze dvě. Zjednodušený přenos klíče pomocí protokolu BB84 je zobrazen na obr. 2.3. Přenos klíče by v tomto případě probíhal následovně: Alice s Bobem se dohodnou na tom, že například polarizace

fotonu pod úhlem 0˚ (↔) nebo 45˚ (↗) bude přiřazovat qubit s hodnotou 0 a polarizace pod uhlem 90˚ (↕) nebo 135˚ (↖) qubit s hodnotou 1 (tab. 2.1).

Tab. 2.1: Dohoda Alice a Boba o volbě fotonů u protokolu BB84

Polarizovaný foton	Hodnota polarizovaného fotonu
↔	0
↕	1
↖	0
↗	1

Alice vygeneruje zcela náhodný klíč, použije sérii náhodných bází a začne s polarizováním a vysíláním jednotlivých fotonů po přenosovém kanálu směrem k Bobovi. Počet fotonů by měl být alespoň dvojnásobně delší než klíč z důvodu možné ztráty přenosem a ověřování chyb. Bob volí také náhodně polarizační bázi a zaznamenává výsledky, které dostal měřením. V případě, že Bob zvolil špatnou bázi, výsledek bude správný s 50% pravděpodobností (obr. 2.3). Po přenesení všech fotonů následuje komunikace Alice s Bobem po nezabezpečeném kanálu. V této části sdělí Bob Alici báze, kterými měřil jednotlivé fotony, ale nikoli jejich polarizaci. Alice odpoví, ve kterých bázích se shodli a ostatní bity klíče „zahodí“ (zhruba 50% z celkového množství). Pokud se Eva snažila odchytit fotony určené Bobovi, taky musela náhodně volit polarizační báze. V případě, že zvolila stejnou jako Alice, k Bobovi se dostanou nezměněné fotony, když ale zvolila nesprávnou bázi, Bob dostal původní fotony jen s pravděpodobností 50 %. Pro případné odhalení Evy budou muset Alice a Bob obětovat ještě několik bitů klíče. U těch si buď sdělí konkrétní hodnoty nezabezpečeným kanálem a pak je zahodí, nebo výsledek předem domluvené operace s obětovanými bity a porovnají je. Při stejných výsledcích by mělo být pravděpodobné, že komunikace nebyla odposlouchávána [25]. Pravděpodobnost, že Eva bude odhalena, je možno vypočítat jako $1 - (3/4)^n$, kde n je počet obětovaných bitů, co je například při 10 bitech 94% úspěšnost. Tento výsledek jsme dostali následujícím myšlenkovým experimentem: jestliže Eva trefila stejnou bázi jako Alice, což je přibližně v 50 % případů, k Bobovi se dostane foton nezměněn. Když bázi neuhodne, polarizace fotonu se naruší a je opět 50% šance, že Bob odměří původní foton. Z toho vyplývá, že při odposlechu Eva způsobí přibližně 25 % chyb. Při zjištění zásahu třetí osoby se klíč nepoužije a začíná celý přenos od počátku.

Obr. 2.3: Princip protokolu BB84 za předpokladu, že Alice a Bob použijí stejnou polarizační bázi

Problém může nastat v případě, kdy si Alice nemůže být jista, jestli je skutečně na druhé straně Bob. K tomuto účelu slouží autentizace. Alice a Bob se na počátku musí dohodnout např. na hesle pro autentizaci. Díky tomuto heslu si můžou být jisti, že komunikují skutečně mezi sebou. Opět tady nastává problém s distribucí, tentokrát hesla, čím jsme se dostali na začátek. Nicméně heslo je možno po každém použití zašifrovat přeneseným klíčem, a tím bychom mohli kvantovou kryptografii nazvat „násobičem“ kryptografie klasické, u které je potřebný přenos klíče neustále opakovat [5].

Protokol BB84 je dnes nejpoužívanějším v kvantové kryptografii. Názorný příklad přenosu klíče vystihuje tabulka 2.2.

Tab. 2.2: Přenos klíče pomocí protokolu BB84

Fáze 1	1	0	0	1	0	1	0	1	0	0	0	1	0	0	1	1	1	1	0
	2	+	×	×	+	×	+	+	×	+	×	×	×	+	×	+	+	×	+
	3	↔	↗	↖	↔	↖	↔	↕	↗	↔	↗	↖	↗	↔	↖	↕	↕	↖	↔
	4	×	×	+	+	×	+	×	+	×	×	+	×	+	+	+	×	×	+
	5	↖	↗	↕	↔	↖	↔	↗	↔	↖	↗	↔	↗	↔	↕	↕	↗	↖	↔
	6	1	0	1	0	1	0	0	0	1	0	0	0	0	1	1	0	1	0
Fáze 2	7		✓		✓	✓	✓				✓		✓	✓		✓		✓	✓
	8		0		0	1	0				0		0	0		1		1	0
Fáze 3	9		0				0											1	
	10		✓				✓											✓	
	11				0	1					0		0	0		1			0

Fáze 1: Kvantový přenos

1. Alice náhodně vygeneruje sekvenci bitů
2. Alice náhodně volí polarizační báze
3. Fotony, které odesílá Alice
4. Bob náhodně volí polarizační báze
5. Fotony, které Bob měřením dostal

6. Převedení fotonů na bity

Fáze 2: Veřejná diskuse

7. Bob sděluje Alici volbu polarizačních bází, ta mu odpoví, ve kterých se trefil
8. Bity Boba, které správně odměřil

Fáze 3: Obětování bitů

9. Obětování bitů pro případné odhalení Evy
10. Porovnání obětovaných bitů
11. Konečný klíč

Úspěšnost protokolu BB84 lze určit vztahem

$$1-\left(\frac{3}{4}\right)^{n}, \tag{2.1}$$

kde n značí počet obětovaných bitů.

2.2 Protokol B92

Tento protokol navrhl v roce 1992 jeden z autorů předešlého protokolu, Charles H. Bennett. Jedná se o dvoustavový protokol, který využívá pouze 2 neortogonální stavy polarizace fotonu, což znamená, že jejich úhly budou navzájem svírat 45˚. Pravděpodobnosti, s jakými je Bob schopen naměřit jednotlivé fotony je zobrazena v tab. 2.3.

Tab. 2.3: Pravděpodobnosti, s jakými Bob měří jednotlivé fotony

Alicini polarizované fotony	Bobovy polarizační báze	Fotony naměřené Bobem	Pravděpodobnost
↔	+	↔	25%
	×	↖	12,5%
		↗	
↖	+	↔	12,5%
		↕	
	×	↖	25%

Celý postup začíná tím, že si Alice zvolí polarizační schémata a bity, sdělí je Bobovi a začne vysílat fotony. V tomto případě si Alice zvolí polarizaci o 0˚ (↔) jako 0 a polarizaci o 45˚ (↖) jako 1, Bob může vyčíst výsledky z přesně opačných polarizací, ↕ jako 1 a ↗ jako 0 (tab. 2.4).

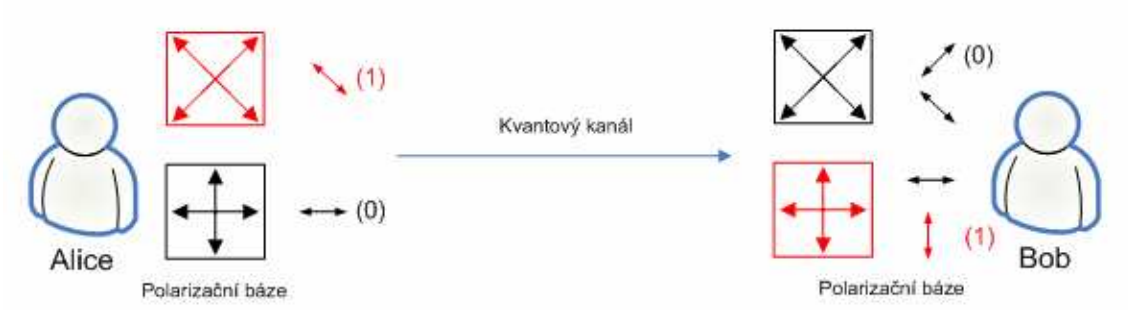
Tab. 2. 4: Dohoda Alice a Boba o volbě fotonů u protokolu B92

Polarizovaný foton	Hodnota polarizovaného fotonu u Boba	Hodnota polarizovaného fotonu u Boba
↔	0	-
↕	-	1
↖	1	-
↗	-	0

Nyní si Alice náhodně vygeneruje klíč, který, už pomocí polarizovaných fotonů, začíná po kvantovém kanálu vysílat Bobovi. Ten náhodně volí polarizační báze a zaznamenává výsledky svých měření. Bob může získat celkem 4 možné výsledky. Tento princip je znázorněn v tab. 2.5. Jestli zvolí stejnou polarizační bázi jako Alice +, tenhle jev nastává s pravděpodobností 50%, Bob není schopen určit hodnotu bitu, protože foton mohl být původně polarizován pod úhlem 0˚, ale i pod úhlem 45˚. Když zvolí opačnou bázi ×, může odchytit foton v podobě ↖, což však nebude brát v úvahu, protože tuto polarizaci zvolila Alice, nebo ↗, a v tomto případě správně změří 0 (tab. 2.5). Z uvedeného vyplývá, že Bob bude schopen odhalit pouze 25% bitů odesílaných Alicí. Bobova vhodně zvolená báze je zakreslená na obr. 2.4. Po odeslání celého klíče nastává komunikace přes veřejný kanál. V tuto chvíli informuje Bob Alici, na kterých pozicích byl schopen fotony identifikovat. Aby zjistili, jestli jejich komunikace nebyla odposlouchávána Evou, řeknou si několik bitů z konečného klíče. Tyto potom zahodí a pro šifrovanou komunikaci použijí klíč, který zůstal utajen [3], [25].

Tab. 2.5: Hodnoty bitů, které je Bob schopen odměřit

Bobova volba polarizační báze	Polarizace fotonu naměřená Bobem	Foton odesílán Alicí	Hodnota bitu
+	↔	↔ nebo ↖	Není možno určit
+	↕	↖	1
×	↖	↖ nebo ↔	Není možno určit
×	↗	↔	0



Obr. 2.4: Princip protokolu B92, kde Bob volí opačnou bázi než Alice

Obrovskou výhodou tohoto protokolu je, že oproti předešlému je podstatně jednodušší pro komunikaci, protože Bob ohlásí jen správně přijaté qubity a lze říci, že je teoreticky zaručeně bezpečný. Prakticky tomu tak není z důvodu větší chybovosti, takže musíme počítat s určitými ztrátami vzniklými ve vlákně, které způsobují složitější odhalení případného útočníka [14].

Jednotlivé kroky přenosu klíče u tohoto protokolu jsou zobrazeny v tab. 2.6.

Tab. 2.6: Přenos klíče pomocí protokolu B92

Fáze 1	1	0	0	1	0	1	0	0	0	0	0	1	0	0	1	1	1	1	0
	2	↔	↔	↖	↔	↖	↔	↔	↔	↔	↔	↖	↔	↔	↖	↖	↖	↖	↔
	3	×	×	+	+	×	+	+	×	×	×	+	×	+	+	+	×	×	+
	4	↖	↖	↔	↔	↖	↔	↔	↗	↗	↖	↕	↗	↔	↕	↕	↖	↖	↔
	5								0	0		1	0		1	1			
Fáze 2	6								✓	✓		✓	✓		✓	✓			
Fáze 3	7								0				0						
	8								✓				✓						
	9									0		1			1	1			

Fáze 1: Kvantový přenos

1. Alice volí náhodné bity
2. Fotony odesílané Alicí
3. Bobova volba polarizačních bází
4. Bobovy výsledky měření
5. Bity Boba, které byl schopen určit

Fáze 2: Veřejná diskuse

6. Porovnání bitů Boba a Alice

Fáze 3: Obětování bitů

7. Obětování bitů pro případné odhalení Evy
8. Porovnání obětovaných bitů
9. Konečný klíč

Pravděpodobnost, se kterou jsme schopni u tohoto protokolu schopni odhalit útočníka, můžeme vypočítat jako:

$$1-\left(\frac{7}{8}\right)^{n}, \tag{2.2}$$

kde n značí počet obětovaných bitů.

2.3 Šestistavový protokol

Méně známý protokol je tzv. šestistavový protokol (SSP). Tento protokol vychází z protokolu BB84, ale, jak už název napovídá, je tady polarizace možná v šesti směrech. Kromě lineární (+) a diagonální (×) polarizace se zde využívá i polarizace kruhová (◯). Z toho důvodu je pravděpodobnost, že Bob neuhodne Alicinu bázi ⅔.

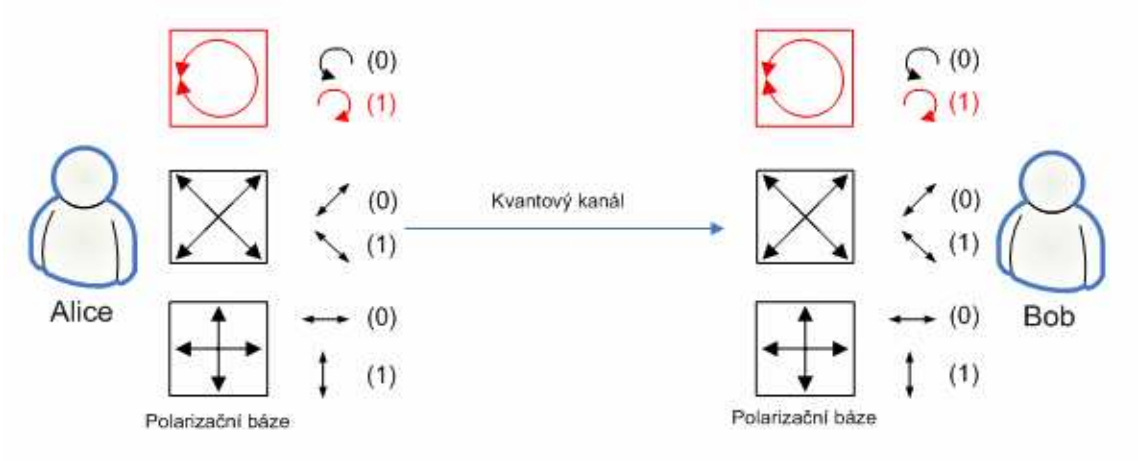
Přenos klíče probíhá podobně jako u BB84: Alice si zvolí qubity, například pro 0 v lineární polarizaci ↔, v diagonální ↗, v kruhové ↺ a pro 1 ↕, ↖ a ↻ (tab. 2.7).

Tab. 2. 7: Dohoda Alice a Boba o volbě fotonů u šestistavového protokolu

Polarizovaný foton	Hodnota polarizovaného fotonu
↔	0
↕	1
↗	0
↖	1
↺	0
↻	1

Nyní mění náhodně polarizace podle vygenerovaného klíče. Bob volí také polarizace podle vlastního uvážení a zachycené bity si zaznamenává. Po ukončení procesu přenosu klíče nastává komunikace přes běžný kanál. Tady nahlásí Bob Alici, v jakém pořadí použil které báze. Alice mu odpoví, ve kterých se shodli a ostatní bity nebudou považovat za součást klíče. Přenos se stejnou volbou polarizační báze vykresluje obr. 2.5. Pro kontrolu ještě obětují několik bitů, aby si byli jisti, jestli do přenosu nezasahovala třetí osoba. Jestli jsou hodnoty obětovaných bitů totožné, Alice s Bobem si podle počtu obětovaných bitů mohou být s určitou pravděpodobností jisti

tím, že jejich komunikace nebyla odposlouchávána. I v tomto případě platí malé procento chyb způsobených kvantovým kanálem [18].



Obr. 2.5: Princip šestistavového protokolu, kde Bob i Alice volí kruhovou polarizační bázi

Názorný přenos klíče pomocí šestistavového protokolu popisuje tab. 2.8.

Tab. 2.8: Přenos klíče použitím šestistavového protokolu

Fáze 1	1	0	0	1	0	1	0	1	0	0	0	1	0	0	1	1	1	1	0
	2	×	○	+	○	×	+	×	×	×	○	+	×	○	+	+	○	×	+
	3	↗	↺	↕	↺	↖	↔	↖	↗	↗	↺	↕	↗	↺	↕	↕	↻	↖	↔
	4	○	×	+	+	○	○	×	○	×	×	+	○	+	+	+	○	×	○
	5	↺	↗	↕	↔	↺	↻	↖	↺	↗	↖	↕	↻	↔	↕	↕	↻	↖	↻
	6	0	0	1	0	0	1	1	0	0	1	1	1	0	1	1	1	1	1
Fáze 2	7			✓				✓		✓		✓			✓	✓	✓	✓	
	8			1				1		0		1			1	1	1	1	
Fáze 3	9							1							1	1			
	10							✓							✓	✓			
	11			1						0		1					1	1	

Fáze 1: Kvantový přenos

1. Alicini náhodně zvolené bity
2. Alicini náhodně zvolené polarizační báze
3. Polarizované fotony odesílané Alicí
4. Volba Bobových polarizačních bází
5. Bobovy zaznamenané fotony
6. Převod fotonů na bity

Fáze 2: Veřejná diskuse

7. Shodně svolené polarizační báze Alice a Boba
8. Shodné bity Alice a Boba

Fáze 3: Obětování bitů

9. Obětování bitů pro případné odhalení Evy
10. Porovnání obětovaných bitů
11. Konečný klíč

Šestistavový protokol je schopen detekovat účast třetí osoby s pravděpodobností

$$1-\left(\frac{2}{3}\right)^n, \tag{2.3}$$

kde n značí počet obětovaných bitů.

2.4 EPR protokol

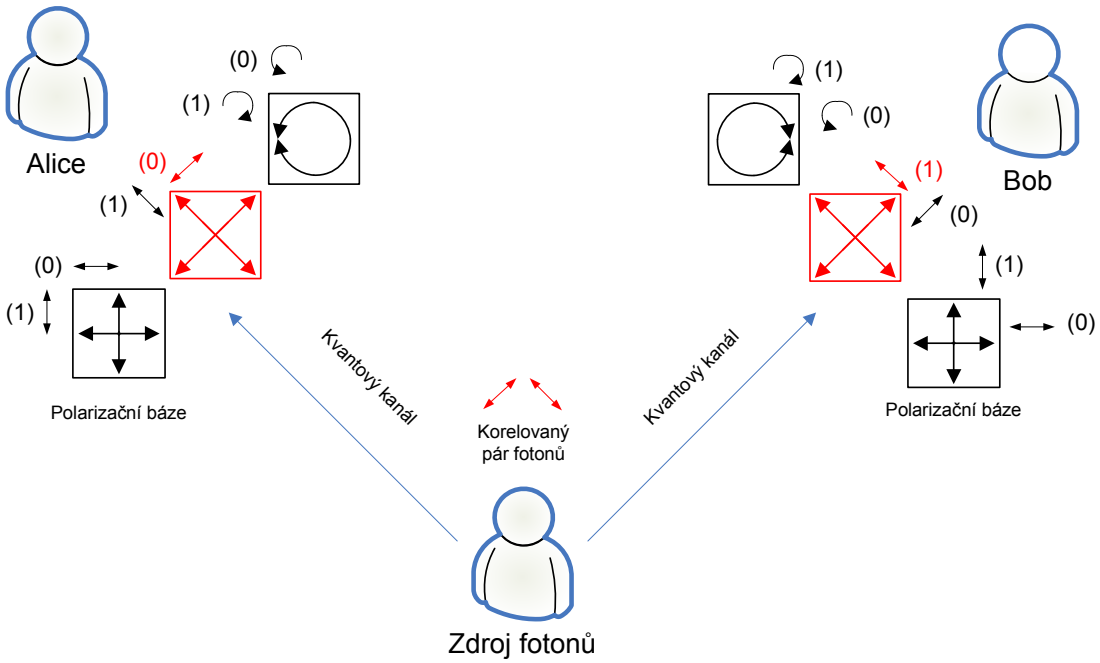
Třístavový protokol EPR navrhl profesor kvantové fyziky Artur Ekert v roce 1991, díky tomu se někdy nazývá protokol E91. Oproti předešlým se liší hlavně tím, že využívá pár fotonů, nikoliv foton v podobě jedné částice. Hlavní výhodou je, že fotonový pár je kvantově provázán a hodnoty měřené veličiny jsou silně korelovány, což znamená, že po naměření jakékoliv polarizace na jedné částici naměříme opačnou polarizaci na částici druhé, i když se fotony nemůžou vzájemně fyzikálně nijak ovlivnit, co je také popsáno díky EPR paradoxu.

U tohoto protokolu probíhá přenos klíče následovně: nezaujatá třetí osoba, přičemž nezáleží na tom, v jaké vzdálenosti je od Boba nebo Alice, vyšle jeden kvantově provázaný pár fotonů. Jeden z páru bude měřen Alicí, druhý Bobem. Alice náhodně volí svou polarizační bázi lineární (+), diagonální (×) nebo kruhovou (○). Bity klíče budou zvoleny např. podle tab. 2.9.

Tab. 2.9: Dohoda Alice a Boba o volbě fotonů u protokolu EPR

Polarizovaný foton	Hodnota polarizovaného fotonu
↔	0
↕	1
↗	0
↖	1
↺	0
↻	1

Jakmile Alice odměří svou část páru, ať už zvolila jakoukoli bázi, na druhé části páru Bob naměří inverzní hodnotu. To tedy znamená, jestliže Bob správně uhodne Alicinu bázi (s pravděpodobností 33%), díky korelaci propojených částic naměří opačnou hodnotu, kterou naměřila Alice. Jestli zvolí nevhodnou bázi, lišící se od té, kterou zvolila Alice, je zde jen 50% pravděpodobnost, že bude mít hodnotu příslušnou k hodnotě Alicina qubitu. Bob tedy také náhodně volí svůj výběr báze. Obr. 2.6 naznačuje přenos klíče se stejně zvolenou polarizační bází. Po odeslání potřebného počtu páru fotonů bude zahájena, stejně jako u předchozích metod, komunikace přes veřejný kanál. Zde si Alice s Bobem sdělí svou volbu báze. Při volbě stejných bází budou tyto bity tvořit klíč, ostatní se použijí pro detekci sledování Evou. Volbou jiné báze dochází k narušení Bellova principu nerovnosti a je dosažena jeho maximální hodnota $2\sqrt{2}$. Jestli se Eva pokusí změřit qubity a odeslat Bobovi jiné, nebo navázat svou částici, dojde buď ke zničení propletenosti páru nebo jeho zeslabení, a úroveň porušení se sníží, co způsobí také snížení hodnoty Bellovy nerovnosti a tím i možnou detekci Evy [15].



Obr. 2.6: Princip protokolu EPR v případě, že Alice a Bob zvolili totožnou polarizační bázi

Chybovost EPR protokolu vypočteme ze vztahu

$$1-\left(\frac{2}{3}\right)^n, \tag{2.4}$$

kde n značí počet obětovaných bitů.

2.5 Protokol SARG04

Čtyřstavový protokol SARG04 nese jméno po svých objevitelích, kterými jsou Valerio Scarani, Antonio Acín, Grégoire Ribordy a Nicolas Gisin, a roku 2004, kdy byl navržen. SARG04 je modifikovanou verzí protokolu BB84, kvantový přenos je u obou totožný, liší se jen ve veřejné diskusi.

QKD začíná tím, že se Alice a Bob dohodnou na hodnotách, které budou jednotlivé polarizace fotonů nést. V tomto případě si zvolí pro polarizaci rovnoběžnou s vertikálou (↕) a pro polarizaci odkloněnou od vertikály o 90˚ (↔) hodnotu bitu 1, a pro polarizace pootočené od vertikály o ±45˚ (↗,↖) hodnotu bitu 0 (tab. 2.10).

Tab. 2.10: Dohoda Alice a Boba o volbě fotonů u protokolu SARG04

Polarizovaný foton	Hodnota polarizovaného fotonu
↔	1
↕	1
↖	0
↗	0

Na začátku distribuce Alice generuje náhodnou posloupnost bitů, které pak náhodně polarizuje a odesílá po kvantovém kanálu Bobovi. Ten volí polarizační báze a zaznamenává si výsledky měření. Po odeslání celkové posloupnosti qubitů následuje veřejná diskuse. V této chvíli Alice neodešle Bobovi volbu svých bází jako u BB84, nýbrž skupinu obsahující dva fotony, které nesmí být vůči sobě ortogonální. Skupiny tedy tvoří následující 4 páry fotonů: (↕, ↗), (↕, ↖), (↔ , ↗) a (↔n, ↖). Jestli je polarizace u Bobova výsledku měření kolmá na polarizaci fotonu u odesílané skupiny, Bob si je jistý, že volba jeho polarizační báze nebyla správná, protože polarizace odeslaného a naměřeného fotonu by musela být totožná. Může teda s jistotou určit, že Alice odesílala druhý foton z tohoto páru. Jestli se Bobův naměřený foton shoduje s jedním ze skupiny, Bob není schopen určit, zda Alice odesílala foton s touto polarizací, nebo byla na Bobově straně špatně zvolená polarizační báze. Všechny možnosti Bobova měření jsou znázorněny v tab. 2.11. Po vyhodnocení Bob sdělí Alici, které bity byl schopen určit. Celý tento průběh ukazuje obr. 2.7. Pro zjištění odposlouchání se obětuje několik bitů, jestli jsou shodné, je veliká pravděpodobnost, že Eva nezasahovala do přenosu a zůstávající řetězec bitů se použije jako výsledný klíč [22], [24].

Obr. 2.7: Princip přenosu klíče pomocí protokolu SARG04

Tab. 2.11: Možnosti Boba určit jednotlivé fotony

Foton polarizo-ván Alicí	Volba Bobovy polarizační báze	Bobova naměřená polarizace fotonu	Podskupin a fotonů odesílána Alicí	Bobovo zjišťování odeslaných fotonů	Hodnota bitu
↔	+	↔	↔, ↗	↔ nebo ↗	Není možno určit
			↔, ↖	↔ nebo ↖	Není možno určit
	×	↖	↔, ↗	↔	1
			↔, ↖	↔ nebo ↖	Není možno určit
		↗	↔, ↗	↔ nebo ↗	Není možno určit
			↔, ↖	↔	1
↕	+	↕	↕, ↗	↕ nebo ↗	Není možno určit
			↕, ↖	↕ nebo ↖	Není možno určit
	×	↖	↕, ↗	↕	1
			↕, ↖	↕ nebo ↖	Není možno určit
		↗	↕, ↗	↕ nebo ↗	Není možno určit
			↕, ↖	↕	1
↖	+	↔	↔, ↖	↔ nebo ↖	Není možno určit
			↕ , ↖	↖	0
		↕	↔, ↖	↖	0
			↕, ↖	↕ nebo ↖	Není možno určit
	×	↖	↔, ↖	↔ nebo ↖	Není možno určit
			↕, ↖	↕ nebo ↖	Není možno určit
↗	+	↔	↔, ↗	↔ nebo ↗	Není možno určit
			↕, ↗	↗	0
		↕	↔, ↗	↗	0
			↕, ↗	↕ nebo ↗	Není možno určit
	×	↗	↔,↗	↔ nebo ↗	Není možno určit
			↕, ↗	↕ nebo ↗	Není možno určit

Tab. 2.12: Distribuce klíče pomocí protokolu SARG04

Fáze 1	1	0	0	1	0	1	0	1	0	0	0	1	0	0	1	1	1	1	0
	2	↖	↗	↕	↖	↔	↗	↔	↖	↗	↗	↕	↖	↗	↔	↕	↔	↔	↗
	3	×	×	+	+	×	+	×	+	+	×	+	×	+	+	+	×	×	+
	4	↖	↗	↕	↕	↖	↔	↗	↔	↕	↗	↕	↖	↔	↔	↕	↗	↖	↔
Fáze 2	5	↔ ↖	↔ ↗	↕ ↖	↕ ↖	↔ ↗	↔ ↗	↔ ↖	↔ ↖	↕ ↗	↕ ↗	↕ ↗	↕ ↖	↕ ↗	↔ ↗	↕ ↖	↔ ↖	↔ ↗	↕ ↗
	6					↔		↔						↗			↔	↔	↗
	7					1		1						0			1	1	0
Fáze 3	8							1									1		0
	9							✓									✓		✓
	10					1								0				1	

Fáze 1: Kvantový přenos

1. Alice volí bity klíče
2. Alicina polarizace fotonů
3. Bobova náhodná volba polarizačních bází
4. Bobovy zaznamenané fotony

Fáze 2: Veřejná diskuse

5. Alice sděluje Bobovi podskupiny fotonů
6. Fotony, které byl Bob schopen určit
7. Převedení fotonů na bity

Fáze 3: Obětování bitů

8. Obětování bitů pro případné odhalení Evy
9. Porovnání obětovaných bitů
10. Konečný klíč

Pravděpodobnost odhalení Evy dostáváme ze vztahu

$$1-\left(\frac{3}{4}\right)^{n}, \tag{2.5}$$

kde n značí počet obětovaných bitů.

3. Současný stav kvantových technologií

Tato část je zaměřená na společnosti a firmy, které buď uvádějí na trh zařízení umožňující kvantovou distribuci klíče, popřípadě kvantové generátory čísel, nebo se zaobírají výzkumem v této oblasti.

3.1 MagiQ Technologies

Soukromá společnost MagiQ Technologies, Inc. vznikla v roce 1999, sídlí v New Yorku a výzkumy provádí v laboratořích ve Smallville, Massachusetts. Zabývá se výzkumem a vývojem v oblasti kvantových technologií, zejména kvantovou kryptografií a komunikací.

V současnosti se zaobírá následujícími oblastmi:

- QKD
- kvantová komunikace
- kvantové šifrování a dešifrování dat
- jednofotonové zdroje a detektory
- laditelné lasery
- optické senzory
- interferometry

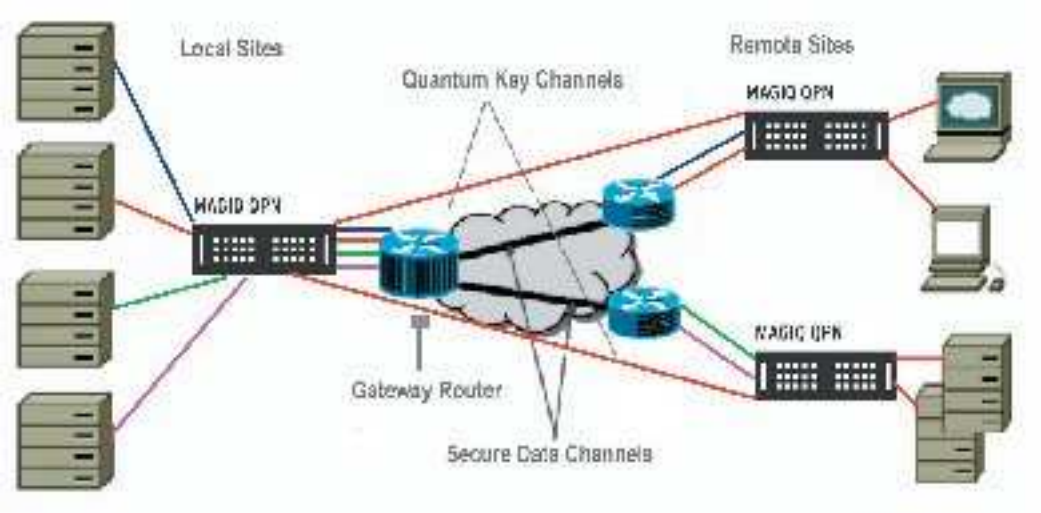
V delším časovém horizontu se společnost hodlá zabývat rozhraním mezi kvantovou pamětí a kvantovou sběrnicí, jednoduchými kvantovými operacemi, algoritmy multiqubitových procesorů a kvantovými informačními technologiemi, např. sestrojením velkokapacitních kvantových počítačů.

3.1.1 QPN 7505

Hlavním produktem společnosti je QPN 7505 (obr. 3.1), který je první komerční „bezpečnostní bránou“ (Security Gateway) pro přenos klíče založenou na principu kvantové kryptografie. Mezi nejdůležitější vlastnosti patří schopnost automatické detekce narušení bezpečnosti, co znamená, že při jakékoliv změně systém okamžitě informuje všechny zúčastněné strany o narušení bezpečnosti. Produkt disponuje také automatickou obnovou šifrovacích klíčů a samozřejmě je odolný vůči pokrokům v informačních technologiích. Klíč využívá pro šifrování protokol BB84, pak je

odesílán po kvantovém kanálu tvořeném běžným optickým vláknem, kterého délka je omezena na 120 km. Pro komunikaci veřejným kanálem přes VPN slouží routery, které používají šifrovací standardy AES nebo 3DES. Celý průběh přenosu je znázorněn na obr. 3.1.

Zařízení je určeno zejména pro finanční ústavy, armádu, vládu a vnitřní bezpečnost, které se zaměřují na nejvyšší úroveň bezpečnosti. Cena základní instalace systému je stanovena od $97000 [23].



Obr. 3.1: Šifrování klíče přístrojem MagiQ QPN a následná výměna dat přes VPN pomocí routerů

Obr. 3.2: QPN 7505 od firmy MagiQ Technologies

3.2 id Quantique

Soukromá společnost id Quantique S.A., jejíž sídlo se nachází v Ženevě, je zaměřená na dvě oblasti, a to síťová bezpečnost a optické přístroje. Poskytuje kryptografické produkty pro poskytovatele služeb, podniky a orgány státní správy.

V oblasti síťové bezpečnosti dodává na trh následující systémy:

- vysokorychlostní přístroj pro šifrování dat využívající QKD - Cerberis
- aplikace pro QKD - Clavis[2]
- vysokorychlostní přístroj pro šifrování dat využívající klasickou kryptografii Centauris
- kvantový generátor náhodných čísel – Quantis

Nabídku v oblasti optických přístrojů tvoří:

- jednofotonové čítače pro viditelnou oblast spektra
- jednofotonové čítače pro infračervenou oblast spektra
- pulzní laserové zdroje

3.2.1 Cerberis

Cerberis (obr. 3.3) je systém, který se skládá ze serveru a šifrovacích zařízení. Využívá vysokorychlostní šifrování kombinované s QKD. Podporuje americký standard AES a šifrovací protokoly BB84 nebo SARG04. Samozřejmostí je i automatická obnova klíče.

Přenos klíče mezi servery je uskutečňován přes optické vlákno, přičemž vzdálenost, na kterou jsou schopny vysílat, je omezena na 50 km. Na požádání je však možno vyrobit i systémy s větším dosahem. Další výměna informací je uskutečňována pouze mezi šifrovacími zařízeními, ty mohou komunikovat přes několik rozhraní: Ethernet (10/100, 1Gbps, 10Gbps), optický kanál (1G, 2G, 3G), SONET/SDH (OC-3, OC-12, OC-48, OC-192) nebo ATM (OC-3, OC-12).

Server je schopen vysílat data hned k několika zařízením souběžně (maximálně 12), přičemž šifrovací zařízení lze vyměnit kdykoli během provozu (Hot Swap).

Obr. 3.3: QKD server s šifrovacími zařízeními Cerberis

3.2.2 Clavis[2]

Tento systém (obr. 3.4) pro QKD je určen zejména pro výzkumné účely v oblasti QC nebo pro implementaci nových síťových protokolů (např. Novell). Dosah je omezen na 50 km. Jsou zde implementovány dva protokoly BB84 a SARG04, pro šifrování se využívá AES nebo Vernamova šifra.

Obr. 3.4: Systém pro výzkumné účely Clavis[2]

3.2.3 Quantis

Kvantový generátor náhodných čísel (QRNG) (obr. 3.5) využívá pro generování čísel zákonů kvantové fyziky, konkrétně kvantových elementárních optických procesů, a všechna čísla jsou dokonale náhodná. Je dostupný ve třech provedeních: jako PCI karta, USB zařízení nebo jako OEM model pro plošné spoje. Princip spočívá v postupném vysílání fotonů na poloprůhledné zrcadlo s tím, že odraz nebo přechod fotonu je zaznamenáván jako binární číslo s hodnotou 0 nebo 1 [13].

Obr. 3.5: Generátor kvantových náhodných čísel jako PCI karta, USB zařízení a OEM model

3.3 SmartQuantum

Mezinárodní společnost SmartQuantum byla založena v roce 2004 a má americkou a evropskou pobočku. Hlavní sídlo společnosti leží v Lannion (Francie), sídlo americké pobočky (SmartQuantum Inc.) se nachází v Houstonu, Texas a evropské společnosti (SmartQuantum S.A.) v Lannion a Paříži. Společnost se zaměřuje na oblast vývoje, výroby a prodeje přístrojů pro přenos tajných dat využívající digitální kryptografii a kvantové technologie. Nabízí také podporu a služby přizpůsobující se průmyslovým, vojenským, finančním a telekomunikačním bezpečnostním požadavkům.

Systémem pro digitální kryptografii je přístroj SQ Cryptor.

Zařízení využívající kvantovou kryptografii jsou:

- SQKey Generator
- SQBox Defender
- SQBox FiberShield – přístroj sestrojen speciálně pro účely francouzské legislativy

3.3.1 SQKey Generator

Přístroj (obr. 3.6) používá zabezpečení klíče pomocí QKD pro stávající systémy digitální kryptografie na trhu. Mezi jeho vlastnosti patří aktualizace klíčů pomocí kvantových technologií a schopnost se kdykoliv autentizovat pro zamezení útoku. Přenos probíhá po optickém vlákně na vzdálenost až 80 km.

Obr. 3.6: Kvantový generátor SQKey Generator

3.3.2 SQBox Defender

SQBox Defender (obr. 3.7) kombinuje distribuci klíče (který též generuje) pomocí QC a přenos dat pomocí digitální kryptografie. Skládá se z modulu pro QKD,

který zařizuje přenos klíče přes kvantový kanál, a šifrovacího modulu, který má za úkol přenášet zašifrované zprávy veřejným kanálem [29].

Obr. 3.7: Zařízení pro kvantový přenos SQBox Defender

3.4 Ostatní firmy a instituce zabývající se kvantovými technologiemi

Vzhledem k faktu, že kvantová kryptografie má zcela určitě obrovskou budoucnost, věnuje se jejímu výzkumu, konkrétně QKD a její implementaci do různých elektronických zařízení, nespočetné množství popředních firem a univerzit, například:

- HP
- TOSHIBA
- IBM
- SIEMENS
- MITSUBISHI
- NTT
- NEC
- Oxfordská univerzita
- Univerzita v Ženevě
- Mnichovská univerzita

V České republice se této problematice od roku 1995 věnuje Univerzita Palackého v Olomouci, kde byl vybudován přístroj pro kvantovou distribuci klíče, i když přenos probíhal jen na vzdálenost 30 cm a s velikou chybovostí.

4. Simulace protokolů kvantové kryptografie

Cílem praktické části bakalářské práce bylo vytvořit program, který by předvedl, jak funguje přenos klíče u jednotlivých protokolů kvantové kryptografie a podrobně popsal jednotlivé fáze tohoto přenosu. K vytvoření simulačního programu bylo k dispozici několik technologií, např. Matlab, C++, Visual Basic, …

Pro tvorbu simulátoru byla zvolena vývojová platforma Flash, konkrétně verze Macromedia Flash MX. Hlavním důvodem rozhodnutí bylo, že Flash není pouze programovací nástroj, ale obsahuje též bohaté grafické funkce, které zjednodušují práci s dynamickými animacemi.

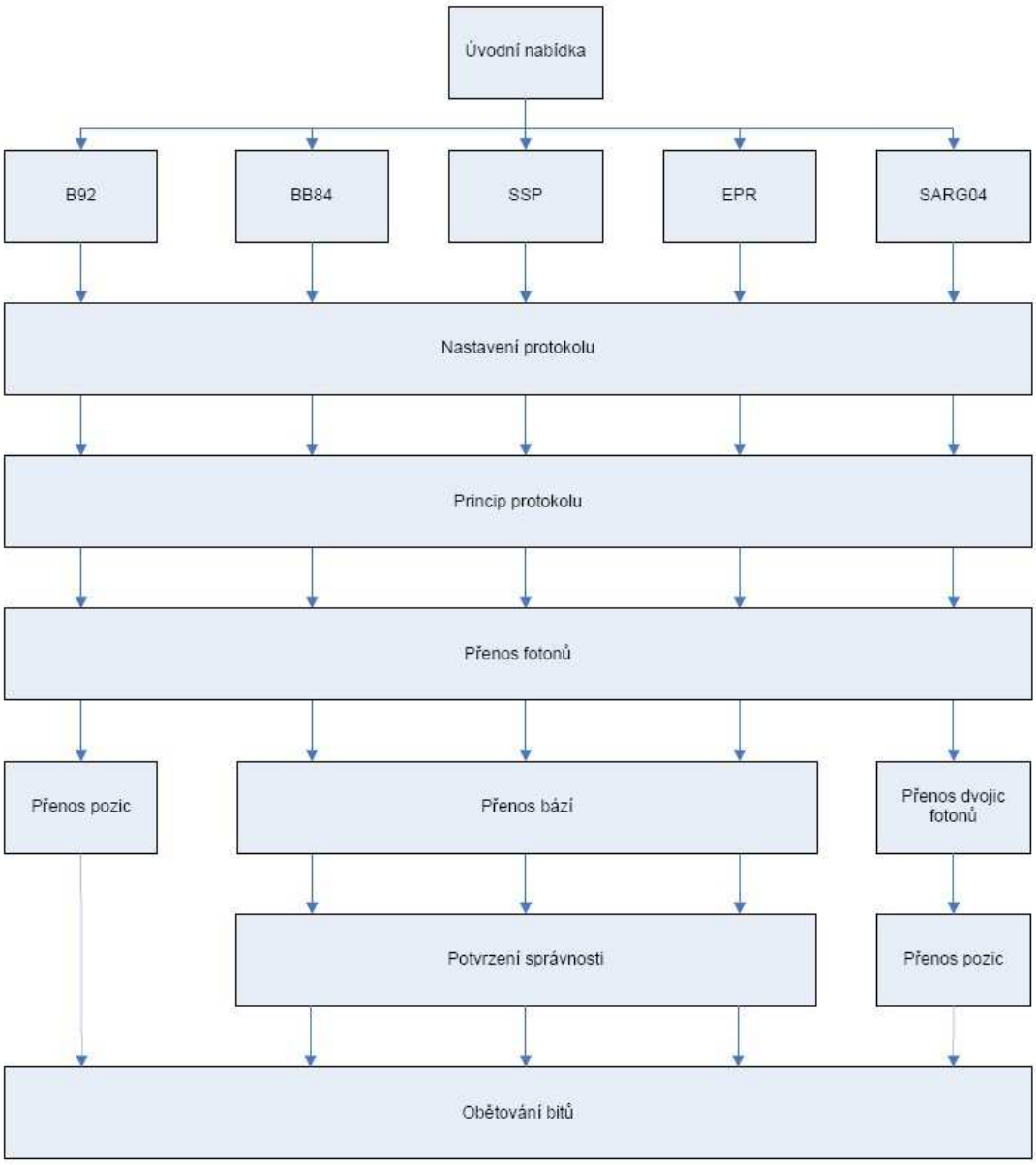
4.1Tvorba simulátoru

Simulační program byl, stejně jako většina jiného softwaru, vytvořen ve třech etapách – návrh, implementace a testování.

Ve fázi návrhu byl simulátor navržen „na papíře“. Konkrétně rozdělení celého programu na jednotlivé simulované protokoly kvantové kryptografie (BB84, B92, SSP, EPR a SARG04), na kroky simulace a rozložení GUI (Graphical User Interface). Stromový diagram celého programu zobrazuje obr. 4.1.

V druhé fázi došlo na samotnou implementaci předchozího návrhu. Prvním krokem byla tvorba struktury programu pomocí snímků a vrstev, které se postaraly o přechody mezi jednotlivými protokoly a kroky simulace. Následovalo vytvoření grafických prvků simulátoru (postavy Alice, Boba a Evy, symboly fotonů, bází a tlačítek) včetně zabudovaných ovládacích prvků (RadioButton, Input Text a Dynamic Text). Posledním krokem implementace simulátoru bylo programování, kterým se grafické prvky uvedou do pohybu a které programu dodá potřebnou funkcionalitu, včetně simulační logiky jednotlivých protokolů. Programovacím jazykem platformy Flash je ActionScript,který umožňuje využití událostmi řízeného spouštění skriptů. Jednotlivé skripty jsou složeny z elementárních příkazů ActionScriptu nebo z uživatelsky definovaných funkcí. Objektově orientované programování (OOP) v ActionScriptu bohužel nelze využít, protože podporuje pouze zabudované objekty, nikoli uživatelsky definované. Všechny části kódu jsou navázány na události tak, aby v pravý čas vykonaly požadovanou akci.

Testování bylo provedeno metodou black-box testing, kdy je program spolu s manuálem předložen k vyzkoušení pokusné osobě, která vyzkouší všechny funkce



Obr. 4.1: Stromový diagram simulačního programu

programu včetně pokusu o uvedení programu do nereálného stavu, např. chybnými vstupy nebo nerespektováním zásad práce se simulátorem. Metoda white-box testing nepřipadala v úvahu kvůli složitého exportu vnitřního stavu.

4.2 Návod pro použití simulačního programu

Jak již bylo zmíněno výše, simulátor byl vytvářen programem Macromedia Flash MX, výstupním souborem se stal Simulator.fla, který byl následně vyexportován do formátu .exe, aby byl spustitelný pod operačním systémem Windows bez potřeby instalace speciálního softwaru.

Tento manuál bude obsahovat podrobný popis pouze 1 kvantového protokolu, a to nejznámějšího a nejstaršího protokolu BB84, většina funkcí je u ostatních protokolů stejná, kromě odlišností, které jsou blíže popsány.

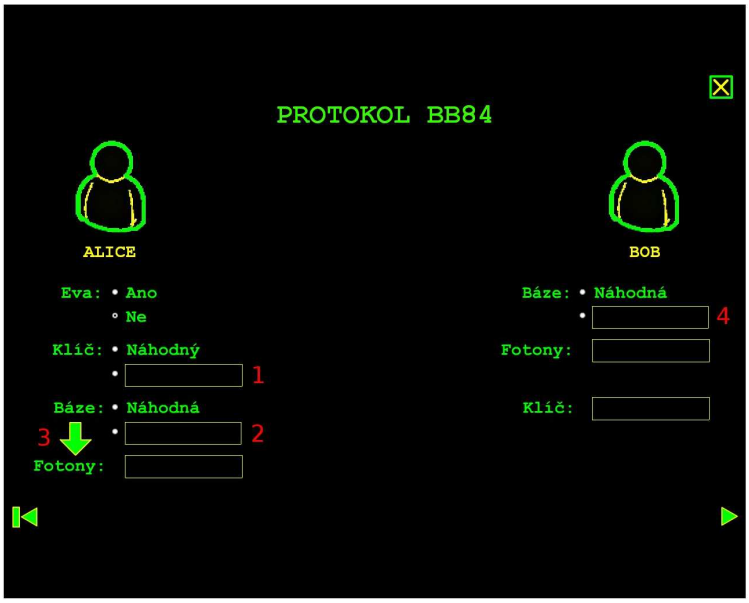
Třístavový EPR protokol v programu využívá pouze stavy 2, z důvodu snadnějšího znázornění samotné podstaty protokolu.

1. Po spuštění programu Simulator.exe se objeví následující úvodní nabídka:

Obr. 4.2: Úvodní stránka simulačního programu

Názvy protokolů jsou zároveň tlačítky, pomocí kterých se dostaneme k jednotlivým přenosům. Tlačítko  provede, stejně jak u běžných programů, ukončení nebo přesněji uzavření aplikace.

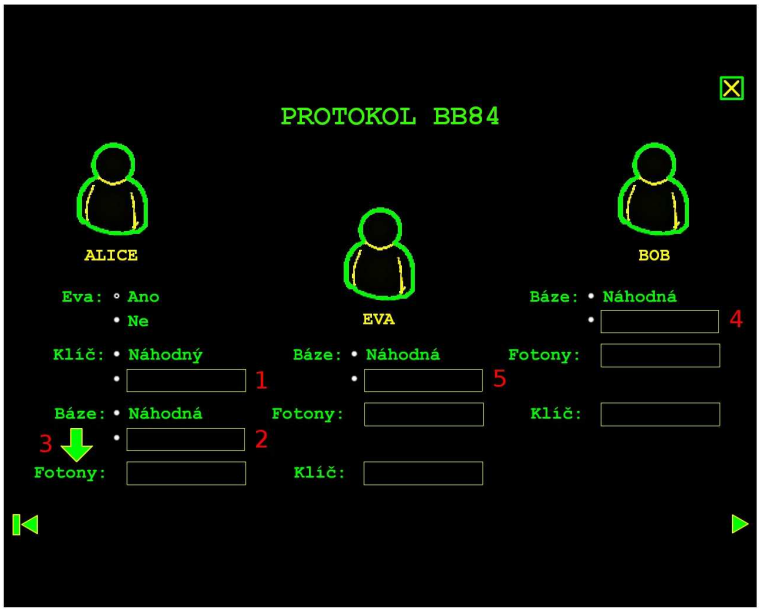
2. Po označení tlačítka „Protokol BB84“ se dostáváme k samotné simulaci.



Obr. 4.3: Vlastní určení parametrů simulátoru u protokolu BB84

Na obrazovce se nachází 2 symboly postav představující Alici a Boba, jakožto uživatele využívající kvantovou kryptografii pro tajný přenos klíče. V případě, že chceme, aby se komunikace zúčastnila i Eva, která by chtěla tuto komunikaci odposlouchávat, označíme přepínač s popiskem „Ano“ u nápisu Eva. V takovém případě se nám na obrazovce objeví i třetí symbol postavy (viz obr. 4.4).

- Protokol EPR obsahuje kromě zmíněných postav ještě jednu, která představuje zdroj fotonů. Ten bude vysílat kvantově provázané fotony k Alici a Bobovi. Zdrojem fotonů není člověk, nýbrž přístroj generující kvantově provázané polarizované fotony. Tato postava je blíže postavená k postavě Alice, protože v tomto případě bude vždy prvním měřícím Alice.



Obr. 4. 4: Vlastní nastavení parametrů u protokolu BB84 za přítomnosti Evy

V této fázi je potřeba vyplnit některá textová pole (na obrázku označené jako 1, 2, 4 a v případě, že byla zvolena i přítomnost Evy, pole číslo 5). Všechny mohou obsahovat maximálně 10 znaků, přičemž v případě, že některé řetězce obsahují méně znaků, program přizpůsobí všechny ostatní akce nejkratšímu z nich. U Alice musíme vyplnit Klíč (označený číslem 1), který může být buď náhodně vygenerovaný, tehdy stačí vybrat volbu přepínače „Náhodně“ u postavy Alice s nápisem Klíč, nebo jej lze doplnit ručně, v tom případě se do vstupního textového pole 1 zapisují číslice „0“ a „1“. Tyto bity tvoří samotný klíč, určeny pro vysílání k Bobovi.

- Textové pole Klíč u Alice se nevyplňuje v případě EPR protokolu, kde uživatelé neurčují posloupnost bitů klíče, ale pouze měří přijatý korelovaný pár fotonů vyslaný třetí stranou.

Možnost Báze (na obr. 4.4 zaznačeny 2, 4 a 5) se nachází u všech tří postav a definuje, jakou bázi chceme fotony buď polarizovat nebo měřit u příjemců. Opět se nabízí možnost náhodného generování nebo vlastního vyplnění tohoto pole, do kterého vepisujeme pouze znaky „+“ a „x“.

Význam jednotlivých znaků:

„+“ – lineární báze

„x“ – diagonální báze

- V případě šestistavového protokolu je možno doplnit ještě znak „o“ s významem

„o“ – kruhová báze

- U protokolu B92 není možnost volby bází u Alice přístupná z důvodu, že polarizace fotonů se určuje pouze podle klíče a předešlé dohody uživatelů. V programu je nastaveno, že Alice může polarizovat pouze fotony ↔ jako 0 a ↖ jako 1. Bob je schopen určit klíč z opačných polarizací těchto fotonů, a to ↕ jako 1 a ↗ jako 0.

- Protokol SARG04 volbu bází u Alice také neobsahuje, protože fotony nejsou polarizovány podle bází, nýbrž podle klíče, u kterého bude polarizace bitu 0 ↖ nebo ↗ a bitu 1 ↕ anebo ↔.

Pro samotné odeslání klíče ze strany Alice v podobě fotonů je ještě potřeba určit polarizaci těchto fotonů podle určeného klíče a báze. Toto se provede automaticky po stisknutí tlačítka  (na obrázcích 4.3 a 4.4 značeno 3), ale pouze v případě, že jsou potřebná pole (Klíč a Báze) vyplněna. Do textového pole Fotony u Alice se vepíšou znaky „|“, „-“, „\“ nebo „/“ podle zvoleného klíče a báze s významem:

„|“ – vertikálně polarizovaný foton (↕)

„-“ – horizontálně polarizovaný foton (↔)

„\“ – polarizovaný foton odkloněný od vertikály o 135˚ ve směru hodinových ručiček (↖)

„/“ – polarizovaný foton odkloněný od vertikály o 45˚ ve směru hodinových ručiček (↗)

- V případě šestistavového protokolu, který má k dispozici navíc kruhovou bázi, může pole obsahovat znaky „)“ a „(“, jenž značí

„)“ – levotočivý polarizovaný foton (↺)

„(“– pravotočivý polarizovaný foton (↻)

Oproti předchozí obrazovce přibyli 2 další tlačítka pro posun v scéně.

 – přechod na úvodní nabídku s výběrem protokolů

 – přechod k následujícímu kroku simulace (ve fázi zadávání vstupních údajů je potřeba mít vyplněné všechna požadovaná pole – Klíč, Báze a Fotony u Alice, Báze u Boba a případně i Báze u Evy)

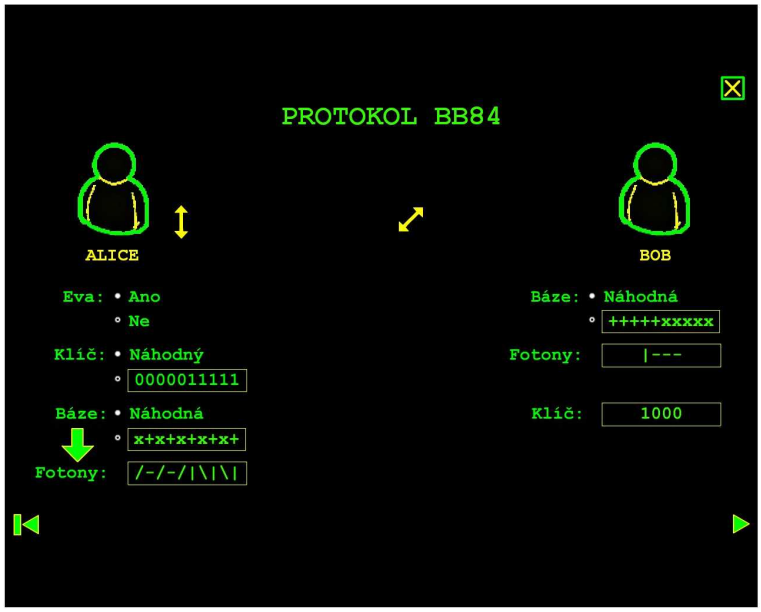
3. Po kliknutí na tlačítko pro přesun k následujícímu kroku se zobrazí tabulka, ve které jsou popsány jednotlivé možnosti při odeslání polarizovaného fotonu a jeho následovní měření pomocí všech typů bází.

Obr. 4.5: Tabulka programu se všemi možnostmi polarizace fotonů a jejich naměření na druhé straně

- U některých protokolů (šestistavový a SARG04) jsou jednotlivé možnosti rozděleny do 2 kroků z důvodu lepší přehlednosti a naznačení všech možných řešení.

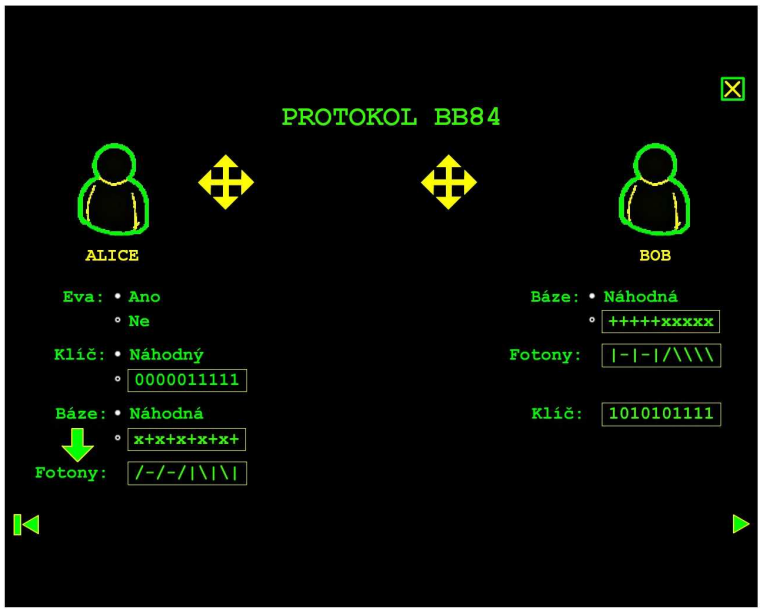
4. V dalším kroku už dochází k samotnému přenosu polarizovaných fotonů směrem od Alice k Bobovi. Ten je měří podle svých předem určených bází a naměřené fotony se postupně zapisují do pole Fotony zobrazeného pod Bobem. Pole Klíč u Boba je vyplňováno bity, které byli získány převodem fotonů do binární podoby podle principů daného protokolu. Jestliže byla předem zvolená i účast Evy, pak fotony směřují nejdříve k ní, ta je podle předem zvolené báze naměří, pomocí fotonů si určí klíč a fotony, které zaznamenala, vyšle směrem k Bobovi.

- Do Bobova pole Klíč u protokolu B92 se vepisují pouze bity, které byl schopen naměřit a určit, tedy pouze v případě že jím naměřený foton je ↕, pak se v poli objeví 1 nebo u ↗ se objeví 0.



Obr. 4.6: Přenos fotonů u protokolu BB84

5. Následuje komunikace přes veřejný kanál. Bob odpovídá v podobě odeslání jím vygenerovaných bází, aby mohl zjistit, ve kterých se s Alicí shodli a ve kterých nikoli.



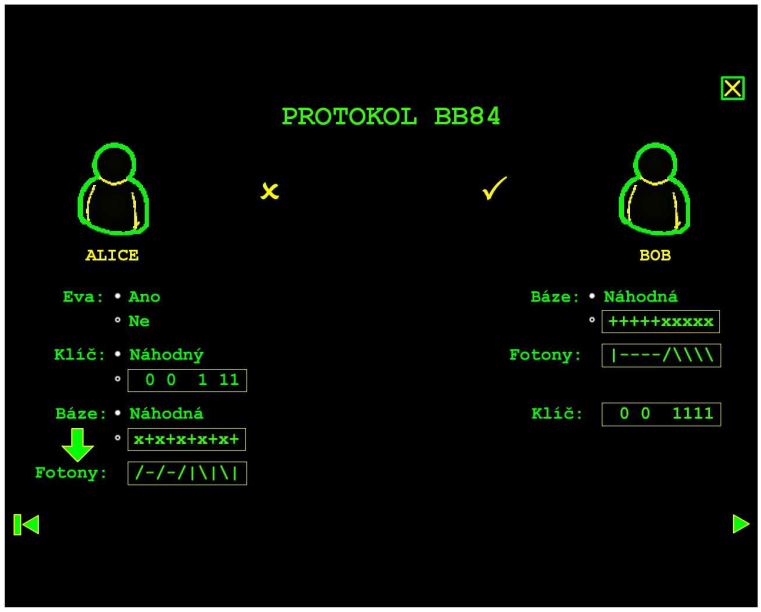
Obr. 4.7: Přenos bází u protokolu BB84

- Změna nastává u protokolu B92, u kterého Bob místo bází odesílá pořadí bitů klíče, které byl schopen určit.

- Báze nejsou vysílány ani u protokolu SARG04. Zde odesílá Alice dvojici fotonů, které nejsou vzájemně ortogonální. Když Bobův naměřený foton je kolmý na jeden z dvojice Alicí odeslaných fotonů, může s určitostí říct, že bázi určil špatně, a tedy

původní foton vysílaný Alicí byl druhý z vyslané dvojice a pomocí tohoto faktu určí bit klíče.

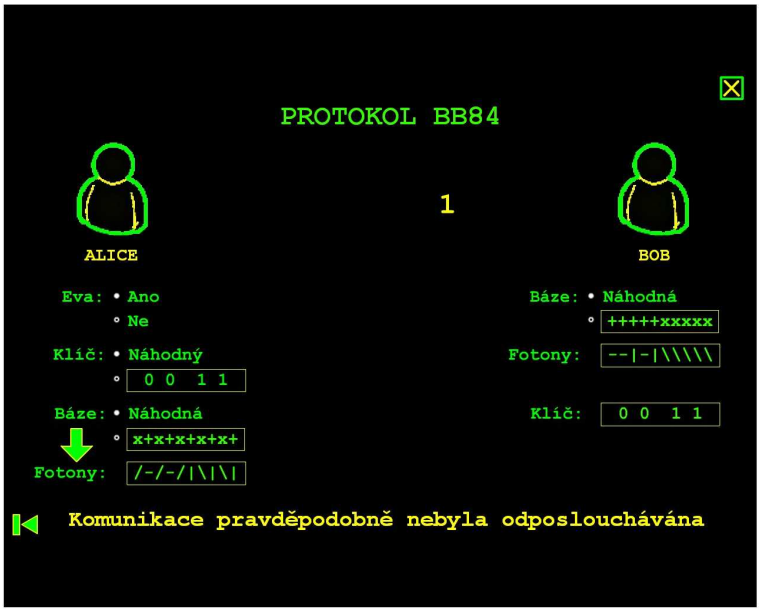
6. Na dalším snímku odpovídá Alice Bobovi znaky ✓ u shody báze a ✗ pokud báze nebyla vhodně zvolena. Při vysílání se u Alice v poli Klíč odmazávají bity u neshody bází a zůstávají pouze bity pravděpodobně stejně naměřené. Totéž se děje na Bobově straně po příchodu uvedených znaků.



Obr. 4.8: Odeslání ověření o správnosti výběru bází

- Tento krok chybí u protokolů B92 a SARG04, protože Alice už podle předchozího bodu mohla s jistotou povědět, které bity byl schopen Bob.

7. Nakonec nastává proces obětování bitů, kdy Alice odešle Bobovi 3 bity (v případě, že klíč obsahuje méně než 3 bity, odešle celý klíč) pro zjištění, jestli komunikace nebyla odposlouchávána. Jestli budou všechny bity shodné, ve spodní části se zobrazí nápis „Komunikace pravděpodobně nebyla odposlouchávána“, v opačném případě se odlišný bit u Boba nahradí vykřičníkem a vypíše se text „Komunikace byla odposlouchávána“. V oznámení o shodě bitů je záměrně použito slovo pravděpodobně, protože shoda 3 bitů z 10 nemusí jednoznačně odhalit přítomnost Evy. Ve skutečném přenosu se odesílají stovky bitů klíče a pro zjištění třetí osoby se obětují desítky bitů. Za takových podmínek je možné s velkou pravděpodobností detekovat odposlech, bohužel v simulačním programu jsou 3 bity příliš málo na odhalení odposlechu.



Obr. 4.9: Konečná fáze přenosu klíče

Závěr

Cílem bakalářské práce bylo popsat metody kvantové kryptografie a následně provést přehled komerčních subjektů zaměřených na tuto oblast. Praktickou částí bylo vytvořit program simulující přenos klíče těmito protokoly, který by bylo možno použít jako výukovou pomůcku.

V první části byly teoreticky popsány jednotlivé protokoly kvantové kryptografie, jejich principy, schémata přenosu klíče a názorné ukázky na jednotlivých příkladech. Byl také vytvořen interaktivní program zobrazující animace samostatných procesů probíhajících při tomto přenosu jednotlivými protokoly. V další části byl proveden souhrn společností zabývajících se kvantovými kryptografickými technologiemi.

Do nedávné doby se systémy kvantové distribuce klíče vyskytovaly pouze jako nákresy na papíře nebo jako prototypy ve vědeckých laboratořích renomovaných univerzit a výzkumných ústavů nadnárodních korporací. I když vývoj na poli kvantové kryptografie započal již před více než čtvrtstoletím, své komerční realizace se dočkala až relativně nedávno, poté, co technický pokrok zapříčinil dostupnost technologií využívaných kvantově-kryptografickými systémy na jedné straně, a v důsledku informačního boomu způsobil nutnost citlivá data chránit na straně druhé.

Působnost prvních několika málo průkopnických firem na trhu s kvantovými kryptografickými zařízeními dává tušit nový směr této vědní disciplíny, která se díky tomu bude rozvíjet jak po stránce teoretické, tak po stránce praktické. Proto lze očekávat další rozvoj na tomto poli, ať už ve výzkumných laboratořích, výrobních střediscích komerčních firem nebo v našem okolí jako záruku soukromí a utajení citlivých informací.

Je však zbytečné podléhat optimismu, protože stejně jako u každé jiné metody kryptografie, se budou zástupy kryptoanalytiků snažit najít chyby a slabiny metody, přičemž u některých QC protokolů již byly nalezeny. Proto nezbývá než nadále vyvíjet nové a zlepšovat již navržené metody QC.

Seznam použitých zdrojů

[1] BRADLER, Kamil. *Kvantová kryptografie – zprávy z přední linie* [online]. 2007 [cit. 2008-11-15]. Dostupný z WWW: <http://www.osel.cz/index.php?clanek=2369>.

[2] BRADLER, Kamil. *Kvantová kryptografie hacknuta!* [online]. 2007 [cit. 2008-11-23]. Dostupný z WWW: <http://www.osel.cz/index.php?clanek=2617>.

[3] CHUNG, Yu Fang, WU, Zhen Yu, CHEN, Tzer Shyong. Unconditionally secure cryptosystems based on quantum cryptography . *Information Sciences* [online]. 2008, vol. 178, is. 8 [cit. 2008-11-16]. Dostupný z WWW: <http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V0C-4R8H1X2-1&_user=640830&_coverDate=04%2F15%2F2008&_alid=825322111&_rdoc=8&_fmt=full&_orig=search&_cdi=5643&_sort=r&_docanchor=&view=c&_ct=1393&_acct=C000032308&_version=1&_urlVersion=0&_userid=640830&md5=9f585aeb11441422efd61b294298092a >.

[4] DUŠEK, Miloslav, CEJNAR, Pavel. Kvantové hlavolamy V. : Bellovy nerovnosti a jejich experimentální testy. *Vesmír : Přírodovědecký časopis* [online]. 1998, roč. 77, číslo 7 [cit. 2008-11-23]. ISSN 1214-4029.

[5] DUŠEK, Miloslav. *Kvantová kryptografie : foton jako důvěryhodný posel* [online]. 2003 [cit. 2008-11-23]. Dostupný z WWW: <https://www.avc-cvut.cz/avc.php?id=2142>.

[6] ENZER, Daphna, et al. *Entangled-photon six-state quantum cryptography* [online]. 2002 [cit. 2008-11-23]. Dostupný z WWW: <http://physics.illinois.edu/research/Highlights/Six-State-NJP.pdf>.

[7] FOTR, Jiří. *Macromedia Flash MX : Podrobná příručka*. Brno : Computer Press, 2004. 358 s. ISBN 80-7226-677-2.

[8] GÜMÜŞ, Ergün, AYDIN, G.Zeynep, AYDIN, M.Ali. QUANTUM CRYPTOGRAPHY AND COMPARISON OF QUANTUM KEY DISTRIBUTION PROTOCOLS. *JOURNAL OF ELECTRICAL & ELECTRONICS ENGINEERING* [online]. 2008, vol. 8, no. 1 [cit. 2008-11-16]. Dostupný z WWW: <http://www.istanbul.edu.tr/eng/ee/jeee/main/pages/issues/is81/81003.pdf>.

[9] HADERKA, Ondřej . *Zdroje a detektory fotonů pro kvantové komunikace* [online]. 2005 [cit. 2008-11-16]. Dostupný z WWW: <http://www.upol.cz/fileadmin/user_upload/PrF-dokumenty/Vedecka_rada/Habilitace_a_profesury/Haderka_Ondrej/Haderka_habilitacni_prace.pdf>.

[10] HÁLA, Vojtěch. Kvantová kryptografie. *Aldebaran bulletin* [online]. 2005, roč. 3, č. 14 [cit. 2008-11-15]. Dostupný z WWW: <http://aldebaran.cz/bulletin/2005_14_kry.php>.

[11] HALLIDAY, David, RESNICK, Robert, WALKER, Jearl. *Fyzika*. Brno : VUTIUM, 2001. ISBN 80-214-1868-0. Moderní fyzika, s. 1033-1054.

[12] HARIHARAN, P. *Basics of interferometry*. 2nd edition. [s.l.] : Academic Press, 2006. 226 s. ISBN 0123735890.

[13] *Id Quantique* [online]. 2006-2008 [cit. 2008-11-30]. Dostupný z WWW: <http://www.idquantique.com/>.

[14] IMRE, Sándor, BALÁZS, Ferenc. *Quantum Computing and Communications: An Engineering Approach*. [s.l.] : John Wiley and Sons, 2005. 283 s. ISBN 047086902X.

[15] JELÍNEK, FARANA. *Kryptografie, kvantová mechanika a jak to souvisí* [online]. 2006 [cit. 2008-11-23]. Dostupný z WWW: <http://fyztyd.fjfi.cvut.cz/2006/cd/prispevky/sbpdf/nevazseII.pdf>.

[16] Katedra fyziky ČVUT v Praze, Fakulta elektrotechnická. *Glosář Aldebaran : Polarizace fotonu* [online]. [2008] [cit. 2008-11-23]. Dostupný z WWW: <http://www.aldebaran.cz/glossary/print.php?id=501>.

[17] KLÍMA, Vlastimil, ROSA, Tomáš. *Kryptologie pro praxi – Agent Foton* [online]. 2006 [cit. 2008-11-15]. Dostupný z WWW: <http://crypto-world.info/klima/2006/ST_2006_05_11_11.pdf>.

[18] KRAUS, GISIN. *Coherent attacks on the six-state QKD protocol* [online]. 2004 [cit. 2008-11-23]. Dostupný z WWW: <www.gap-optique.unige.ch/Projects/Theory/PDF/CohAttacks.doc>.

[19] *Kryptografie* [online]. 2004 [cit. 2008-11-23]. Dostupný z WWW: <http://www.krypto.krokonet.com/>.

[20] KUBÍK, Pavel. *EPR paradox* [online]. 2001 [cit. 2008-11-23]. Dostupný z WWW: <utf.mff.cuni.cz/vyuka/OFY016/F2001/KUBIKPAVEL.DOC>.

[21] KUPČA, Vojtěch. *Kvantová kryptografie* [online]. 2001 [cit. 2008-11-23]. Dostupný z WWW: <http://www.karlin.mff.cuni.cz/~holub/soubory/qc/node25.html>.

[22] LÜTKENHAUS, Norbert. *Photons in Quantum Communication* [online]. 2005 [cit. 2008-12-07]. Dostupný z WWW: <http://nano.physik.hu-berlin.de/HPW/talks/WorkshopPhoton_Lutkenhaus.pdf>.

[23] *MagiQ Technologies* [online]. 2002-2008 [cit. 2008-11-30]. Dostupný z WWW: <http://www.magiqtech.com/>.

[24] MAUERER, Wolfgang, HELWIG, Wolfram, SILBERHORN, Christine. Recent developments in quantum key distribution: Theory and practice. *Annalen der Physik* [online]. 2008, vol. 17, is. 2-3 [cit. 2008-12-07]. Dostupný z WWW: <http://www3.interscience.wiley.com/cgi-bin/fulltext/117905864/PDFSTART>.

[25] NOVÁK, Vladislav. *Kvantová kryptografia*. [s.l.], 2004. 89 s. Slovenská technická univerzita v Bratislave, Fakulta informatiky a informačných technologií . Diplomová práce.

[26] PUŽMANOVÁ , Rita. *Kvantová kryptografie pro bezpečnou distribuci klíčů* [online]. 2004 [cit. 2008-11-15]. Dostupný z WWW: <http://www.lupa.cz/clanky/kvantova-kryptografie-pro-bezpecnou-distribuci-klicu/>.

[27] SHAARI, J.S., LUCAMARINI, M., WAHIDDIN, M.R.B. Deterministic six states protocol for quantum communication . *Physics Letters A* [online]. 2006, vol. 358, is. 2 [cit. 2008-11-30], s. 85-90. Dostupný z WWW: <http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6TVM-4JXRHW2-5&_user=640830&_coverDate=10%2F09%2F2006&_rdoc=1&_fmt=full&_orig=search&_cdi=5538&_sort=d&_docanchor=&view=c&_acct=C000032308&_version=1&_urlVersion=0&_userid=640830&md5=6e8066bc0f550daef41ff08b84fe2a1b#sec002>.

[28] SINGH, Simon. *Kniha kódů a šifer : Tajná komunikace od starého Egypta po kvantovou kryptografii*. Petr Koubský a Dita Eckhardtová. 1. vyd. Praha : Dokořán a Argo, 2003. 382 s. ISBN 80-86569-18-7.

[29] *SmartQuantum* [online]. 2007 [cit. 2008-11-30]. Dostupný z WWW: <http://www.smartquantum.com/-rubrique2-.html>.

[30] SVRŠEK, Jiří. Některé problémy současné fyziky, 5 : EPR paradox a Bellův princip nerovnosti. *Natura* [online]. 1997, roč. 1997, č. 3 [cit. 2008-11-30]. Dostupný z WWW: <http://natura.baf.cz/natura/1997/3/9703-6.html>. ISSN 1212-6748.

[31] VENKATRAMAN, Dheera. *Methods and implementation of quantum cryptography* [online]. 2004 [cit. 2008-11-16]. Dostupný z WWW: <http://dheera.net/sci/qcrypt.pdf>.

Seznam zkratek

3DES – Triple Data Encryption Standard – americký standard vznikající sčítáním algoritmů DES

AES – Advanced Encryption Standard – současný americký standard pro šifrování

ATM – Asynchronous Transfer Mode – asynchronní přenosový mód

B92 – Bennett – název protokolu kvantové kryptografie

BB84 – Bennett, Brassard – název protokolu kvantové kryptografie

DES – Data Encryption Standard – americký standard pro šifrování

EPR – Einstein, Podolsky, Rosen – objevitelé EPR paradoxu

GUI – Graphical User Interface – uživatelské grafické rozhraní

OOP – Object Oriented Programming – objektově orientované programování

PGP – Pretty Good Privacy – šifrovací software

QC – Quantum Cryptography – kvantová kryptografie

QKD – Quantum Key Distribution – kvantová distribuce klíče

QPN – Quantum Private Network – kvantová privátní síť

QRNG – Quantum Random Number Generator – kvantový generátor náhodných čísel

RSA – Rivest, Shamir, Adleman – vynálezci první asymetrické šifry RSA

SARG04 – Scarani, Acin, Ribordy, Gisin – název protokolu kvantové kryptografie

SDH – Synchronous Digital Hierarchy – synchronní digitální hierarchie

SONET – Synchronous Optical Network – synchronní optická síť

SSP – Six State Protocol – šestistavový protokol

VPN – Virtual Private Network – virtuální privátní síť